are based on RFC 2440. The headers involved in the transaction are the "Authorization", "WWWW-Authenticate" and "Response-Key" for providing the user's public key extracted from the pgp key ring.

[0143] Server Discovery

[0144] At this point the SIP provides the server discovery mechanism using pre-defined configuration or multicast queries to a DHCP server. When the user terminal starts up it will immediately obtain the address of its closest SIP server. Another discovery feature also in the SIP protocol is to resolve the nearest SIP server address using the SRV records from DNS.

[0145] Once the use has the server address it can send the SIP REGISTER message containing the SL information in its body. The Registrar server that behaves like the Authentication Server (AUS) required in the SLO architecture will authenticate the initial message. If the contacted SIP server is not a Location Server (LS) the message has a specific header for discovering the Location Server. It will be indicated in the SIP header "Require" sent in the REGISTER message. Hence, for indicating that the incoming message contains Spatial Information and needs to be processed by a Location Server, the SIP REGISTER will have the following header: "Require: SLO-server". It indicates that the user is registering his location and needs a Spatial Location Server to manage this data. In case that the server contacted has no SL capabilities the user will receive back a response where the "Contact:" header includes the address of the new SIP server, which can handle that message. An example would be like this: "Contact: slo-server.nokia.com".

[0146] Once the user has contacted the SIP Register the client should start the registration where it will include the SLO in the payload.

[0147] Afterwards, the user knows the address of the Registrar where he can send the request, which includes the SLO data. Now, it is necessary to establish a secure transaction for providing the information to the Registrar. The SIP will handle the security of the transactions during the registration based on the mechanism described in the above "Security Mechanism" section.

[0148] The whole process is depicted in **FIG. 7B** which shows the different steps till the registration succeeds. The messages **1** and **2** are just the SIP server discovery independently of whether it is SLO capable or not. The messages **3** and **4** are sent when the user is trying to register the SLO information in the SIP Registrar but unfortunately, for the illustrated example, it does not have SLO capabilities. Instead, the response **4** indicates the location of the closest SIP sever that can handle a SLO message. Finally, in the messages **5** and **6** the registration is achieved and the SLO data is stored in the SLO server which can be accessed for any other services using SIP or any other Directory Access Protocol.

[0149] Representation Negotiation

[0150] After being contacted the Spatial Location server performs a representation negotiation. The SLO architecture has a default format but it should understand other formats that will be previously negotiated. In case the information received cannot be interpreted or it is coming from non IP device, the SLO server will need to contact a Spatial Location Gateway (SLG) to translate the information received in the SIP payload. Finally, if there is no way for the SLO server to handle the message, it will send back an error SIP message like: "SIP/2.0 501 Not Implemented" or "SIP/2.0 503 Service not available".

[0151] Since the SLO is a new service, it remains a possibility that the contacted SIP registrar does not support this feature. There are two possibilities, the first one is trying to register with the closest SIP Registrar and wait for its response, and the other solution would be to use the OPTIONS message for querying beforehand the Registrar's capabilities. In the former case, if the registrar can handle a SLO message the registration will succeed, otherwise the User Agent receives a 300 response with the address of a SLO enabled SIP Registrar. In the other case, the User Agent needs to negotiate this capability with the registrar. The client will send an OPTIONS message to the registrar for indicating that he needs a SLO based registrar. The registrar can send back a 200 OK response, which means that it can manage this type of registration. Otherwise, the registrar returns a 300 Multiple Choices response, which means that the requested capability can be accessed through the proxy given by the "Contact:" field.

[0152] Scenarios

[0153] Scenarios can be envisioned such as described in IETF draft-polk-slp-loc-auth-server-00.txt entitled "ISL Architectural Considerations" Mar. 8, 2000 by S. Nyckalgard and J. Loaghney. Basically, SIP based devices have to be differentiated from general IP appliances.

[0154] First of all a lookup is needed for finding the Server to which the messages will be addressed. As mentioned above, the Target can use a multicast mechanism for searching for the closest Location Server to its actual location. In case of an SIP enabled device it will use the SIP server discovery mechanism already described.

[0155] The Target is by default an IP based device and during this phase the Target will provide its new assigned address and its device capabilities to the Location Server. The LS will respond to the Target either with its own address in case that satisfies the user device requirements or it will give back the address of the Location Proxy Server that will be able to translate the Target requirements to the standard message format of the protocol. The Location Server or the Location Proxy Server (LPS) will thus be the entity that will take care of this first contact with the Target according to the decision taken after the Representation Negotiation phase.

[0156] If the Proxy server takes care of this phase it will be necessary to maintain a cache of the specific Location Server that has the user profile. Those caches would be updated and replicated among the different proxies to be aware of the respective LS that handle the information of each Target (Authorization, billing, etc.) See J. Luciani et al, "Server Cach Synchronization Protocol (SCSP)" IETF RFC 2334, April, 1998.

[0157] After the LPS has been discovered the Target will start the Negotiation phase. On one side the Target will provide its identification and service requirements to the LPS and in the other side the Proxy (based on its cache table) will contact the Location Server that handles the private information of that user. The LPS will receive back an acceptance from the LS, or not, in case of denial of service for that user.